

# AI-Enabled Biometrics

*in the Age of Generative Intelligence*

**Professor Dinh Phung**

Research Director, Dept. of Data Science and AI, Monash University

[dinh.phung@monash.edu](mailto:dinh.phung@monash.edu)

**Professor Joanna L Batstone**

Director, Monash Data Futures Institute

**AI and Biometrics: Harnessing Potential, Managing Risk**  
Joint ATSE - Victorian Parliamentary Library Webinar  
Melbourne, 19<sup>th</sup> October 2023

# From 'being' to biometrics data



“During the first day of a baby life, the amount of data generated by humanity is equivalent to 70 times the information contained in the library of congress”  
 – book “The Human Face of Big Data”

## Biological data



## Behavioural data

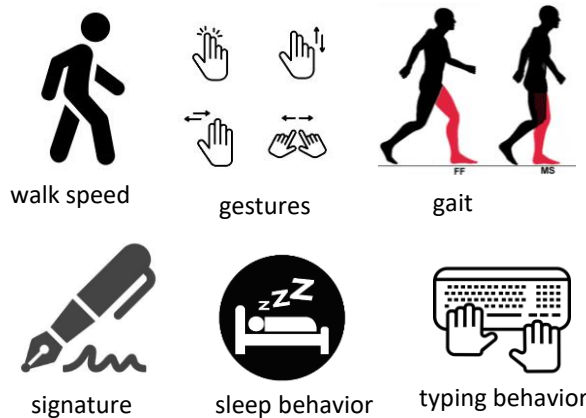
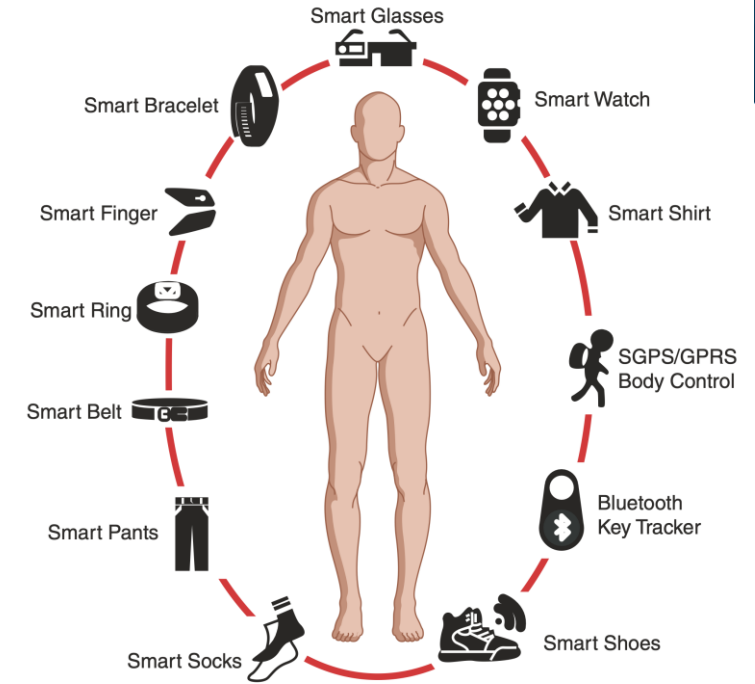


Image credit: IsHak, Waguih William, et al. "The Future of Psychiatry." *Atlas of Psychiatry*, 2023



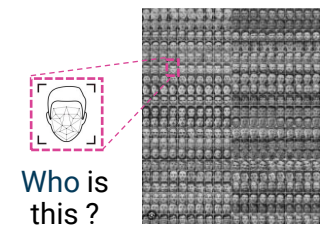
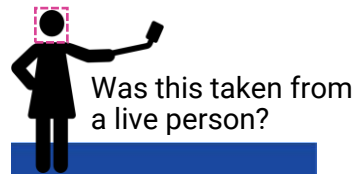

Unprecedented ability to capture biometrics data

Revolution in wearable sensing technology




# Biometrics authentication systems

## Few useful concepts – AI-enabled eKYC example


**SELFIE-ID MATCH**

Match customer IDs to customers with high accuracy




**LIVENESS CHECK**

Guard against spoofing attempts by checking for a live customer




**ID OCR**

Extract details of ID to pre-populate forms for simplified user onboarding



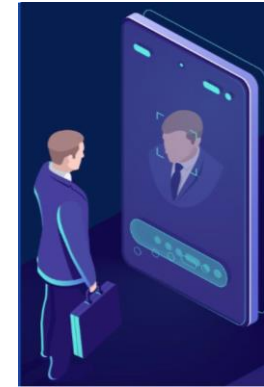
**IDCHECK**

Check ID cards to determine discrepancies or tampering

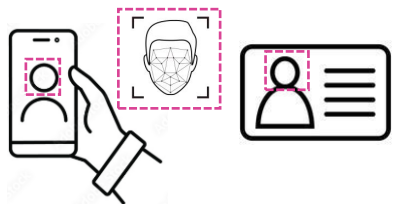


**FACE RETRIEVAL**

Check a customer face against a database of millions of faces in milliseconds



**Recognition**  
compare the identity/face



**Detection**  
detect type of biometric signals (e.g., face)

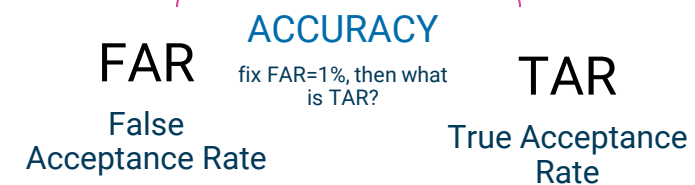


OCR, **information extraction** from claimed ID document

Is this ID document **real**?



**Authentication onboarding**



# RECOGNITION

vs

# INSIGHT ANALYSIS



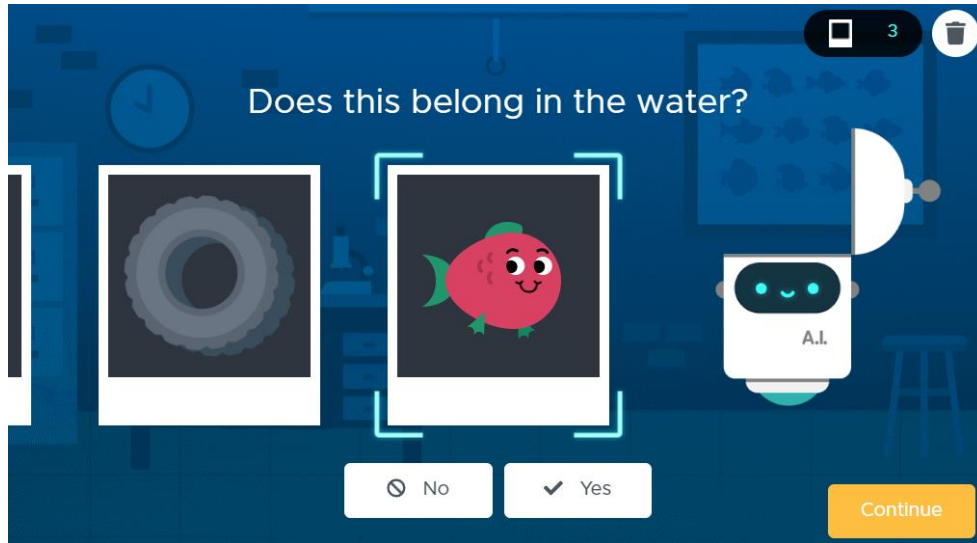
unlocking our smart phone, airport smart gates,  
secure building entry, bank digital ID verification,  
finding lost children, face-recognition surveillance



health/vital sign signals, anger, feelings,  
sentiments, honesty, sexual orientation,  
visual focus, engaged, drowsiness, sleepy,  
etc.

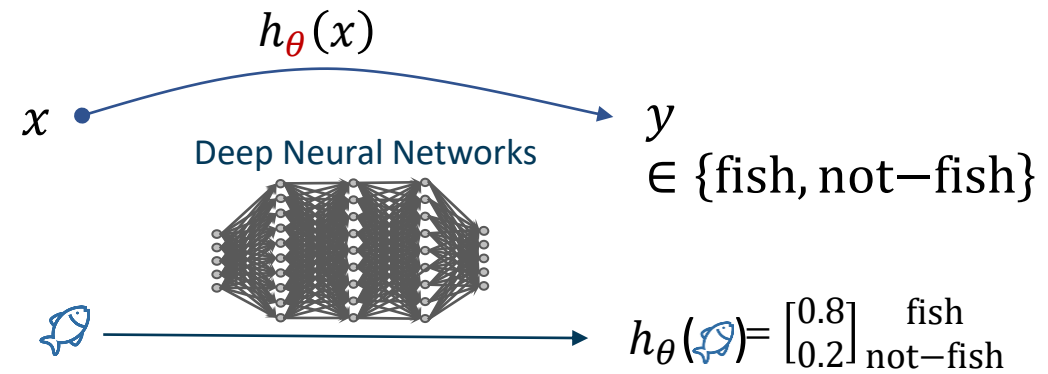
Have far more unexplored scientific values!

# How machine learns?



"AI for Ocean", <http://studio.code.org>

1. Collect data
2. Label data
3. Train model
4. Deploy
5. Repeat



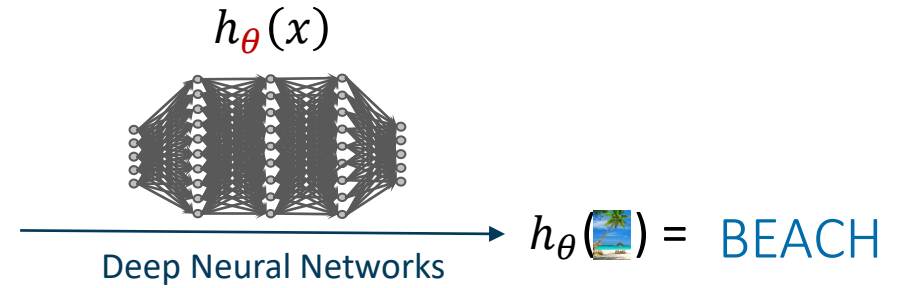
Until 2022 ....

AI = Narrow AI =  
Machine/Deep Learning  $\approx$  Recognition

# What's generative intelligence?

Until 2022 ....

AI = Narrow AI =  
Machine/Deep Learning  
 $\approx$  Recognition



# What's generative intelligence?

~~Until 2022 ....~~

~~AI = Narrow AI =~~  
Machine/Deep Learning  
 $\approx$  Recognition  
+ Generation



$$h_{\psi}^{-1}(y = \text{beach})$$

'Reverse' Deep Neural Networks

BEACH

# What's generative intelligence?

~~Until 2022 ....~~

~~AI = Narrow AI =~~  
Machine/Deep Learning  
≈ Recognition  
+ Generation



$$h_{\psi}^{-1}(y = \text{beach})$$

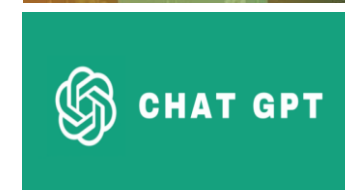
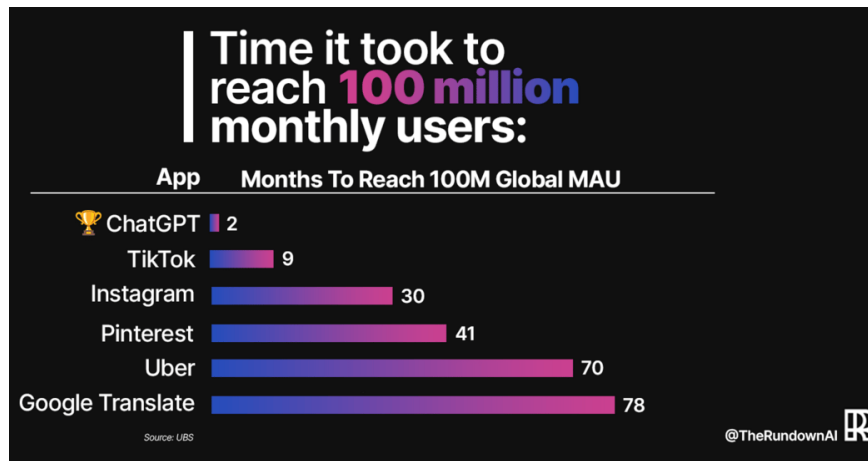
'Reverse' Deep Neural Networks

BEACH

Generative models learn how data is generated to re-generate new data.

## 2022 – 2023: years of Generative AI

Auto-Encoding Variational Bayes	VAE	Key research/technology
Diederik P. Kingma Machine Learning Group Universiteit van Amsterdam		
Max Welling Machine Learning Group Universiteit van Amsterdam		
Generative Adversarial Nets	GAN	
Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, Yoshua Bengio Département d'informatique et de recherche opérationnelle		
Denoising Diffusion Probabilistic Models	Diffusion	
Jonathan Ho UC Berkeley jonathanho@berkeley.edu		
Ajay Jain UC Berkeley ajayj@berkeley.edu		
Pieter Abbeel UC Berkeley pabbeel@cs.berkeley.edu		
Attention Is All You Need	Transformers	
Ashish Vaswani* Google Brain		
Noam Shazeer* Google Brain		
Niki Parmar* Google Research		
Jakob Uszkoreit* Google Research		



<https://www.therundown.ai/p/chatgpt-becomes-fastest-growing-consumer-app-history>



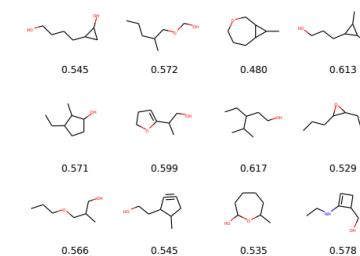
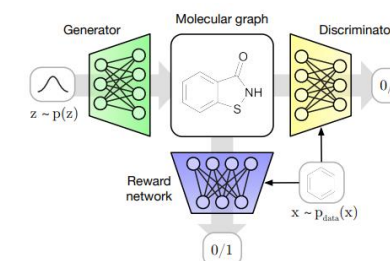
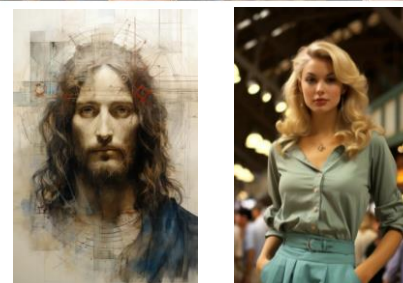


To generate, models need to acquire the ability to **'internalise'** and **'understand'** the world.



from his travels it might have been  
 from his travels it might have been  
 from his travels it might have been  
 from his travels it might have been  
 from his travels it might have been  
 from his travels it might have been  
 from his travels it might have been  
 from his travels it might have been

[Graves '13]



MoIGAN

ARTIFICIAL INTELLIGENCE

## OpenAI's new language generator GPT-3 is shockingly good—and completely mindless

The AI is the largest language model ever created and can generate amazing human-like text on demand but won't bring us closer to true intelligence.

By Will Douglas Heaven

July 20, 2020



Not only can algorithms generate nice photos, videos, codes and human-level texts, but also handwritten, signature, voice, molecular, etc

# Rethinking Biometrics Technology

## in the Age of Generative Intelligence

What if machines are so good at 'generating' fake biometrics signals?



### We Broke Into A Bunch Of Android Phones With A 3D-Printed Head

Screenshot taken from [Forbes](#)



We 3D Printed Our Heads To Bypass Facial Recognition Security And It Worked

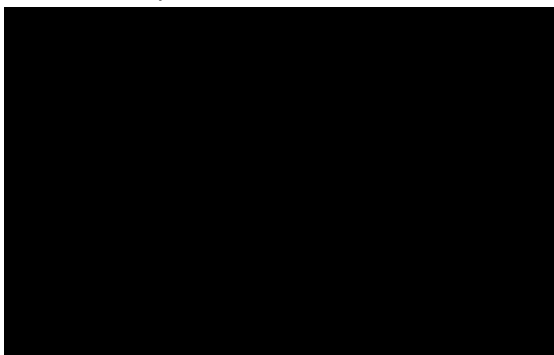
WATCH 4:24

LG G7 ThinQ, a Samsung S9, a Samsung Note 8 and a OnePlus 6

> ARTIFICIAL INTELLIGENCE

### Seeing Isn't Believing: This New AI System Can Create "Deep Fake" Videos

By Glenn McDonald



### AI 'voice clone' scams increasingly hitting elderly Americans, senators warn

'Imposter' scams cost Americans about \$2.6 billion each year

### AI voice cloning scams 'will come to Australia' - so how do you guard against it?

Video taken from [The Guardian](#)

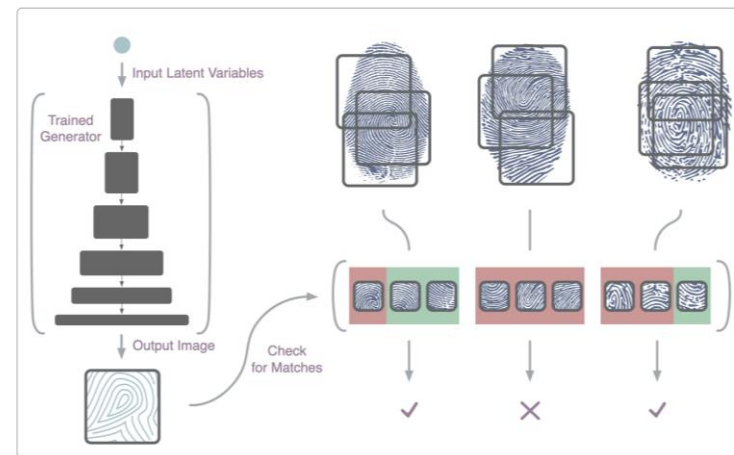


"only need 3 seconds to clone your voice"



AI can fool voice recognition used to verify identity by Centrelink and Australian tax office

Video taken from [The Guardian](#)



Latent Variable Fitness Function

Bontrager et al. (2018)

From NY Uni and Michigan State Uni:

- Can bypass locks on cell phones
- TAR=77% at FAR=1%

# Final Remarks

So, what's next?



- Face recognition becomes so accurate. **It will continue to be so for other signals as well**, use-cases are everywhere!
- **Analysis/Insights has unlimited scientific values** –
- Maybe, for the first time, we can do 'surgery' on our behaviours, hence helps with medical understanding, health, mental health, suicide prevention, car accidents, etc.



- **Without timely research and technology, it could be impossible to tell** who is who or if the data is actually 'biometrics' data or just fake.
- It might **invalidate** many existing technologies today.
- A **radical/rethinking**, a **reboot** to biometrics authentication might be required.



- **Ensure** responsible use of AI.
- **Enforce** traceability and accountability for Generative AI technology.
- **Enhance** current and future AI capability.



**THANK YOU**

[dinh.phung@monash.edu](mailto:dinh.phung@monash.edu)

# Appendix

# Adversarial Attack and Robustness

- **Deliberately exploit** loopholes in the AI system to disrupt its functions
- Deep learning: turns out, it's very easy to **hack** DNNs!

Panda

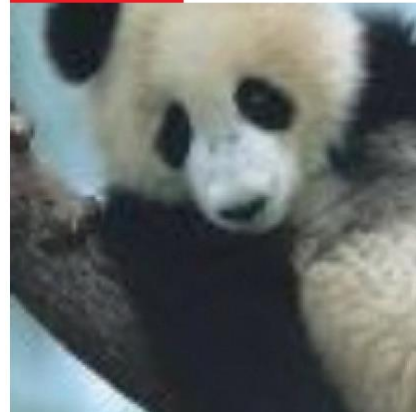


+



→

Gibbon



$\epsilon$ - small perturbation

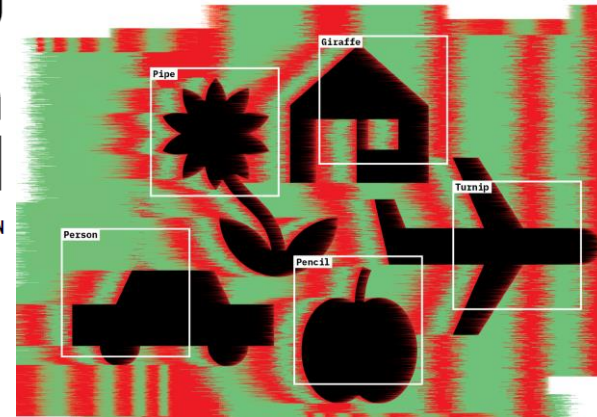
Heaven D., *Deep Trouble for Deep Learning*, Vol 574 *Nature*, 2019.

ILLUSTRATION BY EDGAR BAYK

## DEEP TROUBLE FOR DEEP LEARNING

BY DOUGLAS HEAVEN

ARTIFICIAL-INTELLIGENCE RESEARCHERS ARE TRYING TO FIX THE FLAWS OF NEURAL NETWORKS.



10 OCTOBER 2019 | VOL 574 | NATURE | 163

# Adversarial Attack and Robustness

- Deliberately exploit loopholes in the AI system to disrupt its functions
- Deep learning: turns out, it's very easy to **hack** DNNs!

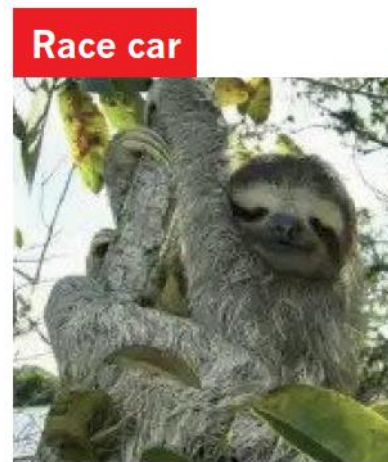
## Targeted Attack



+



→



Heaven D., *Deep Trouble for Deep Learning*, Vol 574 *Nature*, 2019.

ILLUSTRATION BY EDGAR BAYK

## DEEP TROUBLE FOR DEEP LEARNING

BY DOUGLAS HEAVEN

ARTIFICIAL-INTELLIGENCE RESEARCHERS ARE TRYING TO FIX THE FLAWS OF NEURAL NETWORKS.



10 OCTOBER 2019 | VOL 574 | NATURE | 163

# Examples on misuse of GenAI in biometrics and more ...

## FTC issues warning on misuse of biometric info amid rise of generative AI



Screenshots taken from [Fox News](#) and [9News](#)

ARTIFICIAL INTELLIGENCE

## AI 'voice clone' scams increasingly hitting elderly Americans, senators warn

'Imposter' scams cost Americans about \$2.6 billion each year

AI voice cloning scams 'will come to Australia' - so how do you guard against it?

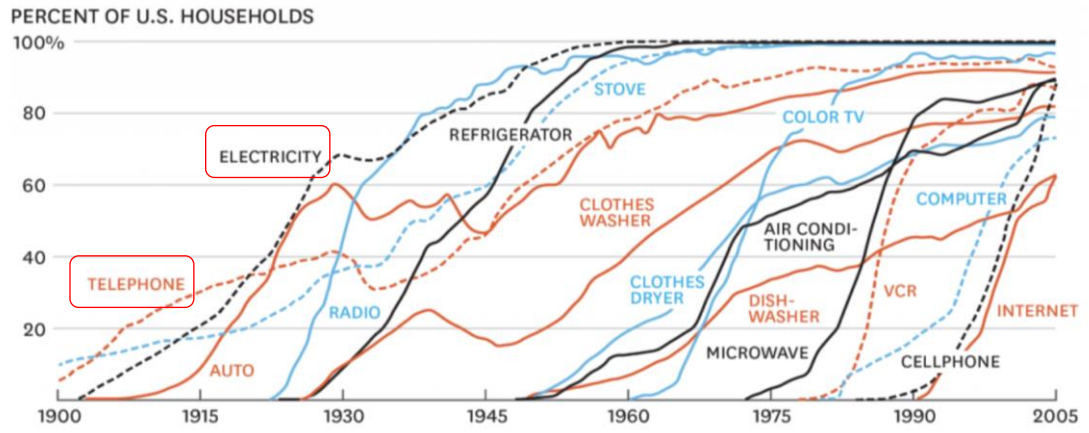




! World adoption of previous technology took **decades**.

🔧 Recent adoption is measured in **months**.

**CONSUMPTION SPREADS FASTER TODAY**



SOURCE NICHOLAS FELTON, THE NEW YORK TIMES HBR.ORG

© innovation copilots 2022

